

PL



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/780,037	02/09/2001	Robert P. Wright	MAC1027U	8437
25197	7590	08/25/2004	EXAMINER	
LEARY & ASSOCIATES 3900 NEWPARK MALL RD. THIRD FLOOR, SUITE 317 NEWARK, CA 94560			DINH, MINH	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 08/25/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/780,037

Applicant(s)

WRIGHT ET AL.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 February 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-13 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: the specification refers to Figure 1 (p. 21, line 25); however, there is no Figure 1, only Figures 1(a) and 1(b).

Appropriate correction is required.

Claim Objections

3. Claims 8 and 13 are objected to because of the following informalities: the limitation in steps (dd) and (ff) of claims 8 and 13 respectively "decrypting the encrypting the data document in step (j)". The limitation is interpreted as "decrypting the encrypted data document in step (j)" in both claims. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2132

5. Claims 5 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 5, it recites the limitations "step (k)" (1st line) and "step (l)" (3rd line). Claim 5 depends on claim 3, which depends on claim 1; however, these limitations are not recited in the parent claims. The claim is treated as being a dependent claim of claim 4.

b. Regarding claim 7, it recites the limitations the hashing applet (1st and 4th line). There is insufficient antecedent basis for this limitation in the claim. The claim is treated as being a dependent claim of claim 6.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (6,154,543) in view of Hickman (6,173,332).

a. Regarding claim 1, Baltzley discloses a method comprising:

(a) linking a first local terminal to a server via the network (fig. 6, 115);

Art Unit: 2132

(b) signaling to the server from the first local terminal that a secure transmission of a data document resident on the first local terminal is desired (fig. 6, 115);

(c) downloading an encryption program resident on the server into random access memory on the first local terminal (fig. 6, 610; col. 2, lines 37-40);

(d) encrypting the data document using the encryption program to create an encrypted data document on the first local terminal (fig. 6, 630);

(e) uploading the encrypted data document from the first local terminal to the server via the network (fig. 6, 115);

(f) linking a second local terminal to the server via the network (fig. 8, 110);

(g) signaling to the server from the second local terminal that a secure transmission of the encrypted data document on the server is desired (fig. 8, 110);

(h) downloading the encrypted data document from the server to the second local terminal (col. 7, lines 24-28);

(i) downloading a decryption program resident on the server into random access memory on the second local terminal (col. 7, lines 24-28; col. 2, lines 37-40); and

(j) decrypting the encrypted data document using the decryption applet to recreate the data document on the second local terminal (col. 7, lines 24-28).

Baltzley does not disclose that the downloaded encryption/decryption program is an applet. Hickman discloses programs known as applets being downloaded and run on a user's computer (col. 2, lines 44-50). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method

Art Unit: 2132

such that the encryption/decryption program is an applet, as taught by Hickman, because applets are machine independent.

b. Regarding claim 2, Baltzley discloses that step (a) further comprises authentication of the first local terminal (col. 5, lines 65-66) and step (g) further comprises authentication of the second local terminal (col. 5, lines 65-66; col. 6, lines 53-67).

c. Regarding claim 3, Baltzley further discloses that steps (b), (c), (d) and (e) are initiated and carried out by a single command from the first local terminal, and steps (g), (h), (i) and (j) are initiated and carried out by a single command from the second local terminal (fig. 6, 605 and 610; col. 2, lines 37-40).

d. Regarding claim 4, Baltzley does not disclose that the method of claim 1, further comprising: (k) deleting the encryption applet from the random access memory on the first local terminal; and (l) deleting the decryption applet from the random access memory on the second local terminal. Hickman discloses the applet being deleted from the terminal on termination of the applet (col. 2, lines 55-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method such that it further comprises (k) deleting the encryption applet from the random access memory on the first local terminal; and (l) deleting the decryption applet from the random access memory on the second local terminal, as taught by Hickman. Please refer to motivation recited for using applets as taught by Hickman in claim 1.

e. Regarding claim 5, Baltzley discloses that steps (b), (c), (d) and (e) are initiated and carried out by a single command from the first local terminal, and steps (g), (h), (i) and (j) are initiated and carried out by a single command from the second local terminal (fig. 6, 605 and 610; col. 2, lines 37-40). Baltzley does not explicitly disclose that step (k) is initiated and carried out by the same single command from the first local terminal, and step (l) is initiated and carried out by the same single command from the second local terminal. Hickman discloses the applet being automatically deleted from the terminal on termination of the applet (col. 2, lines 55-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method such that the deletion of the applet is automatically done on termination of the applet, as taught by Holloway. Accordingly, steps (b), (c), (d), (e) and (k) are initiated and carried out by a single command from the first local terminal, and steps (g), (h), (i), (j) and (l) are initiated and carried out by a single command from the second local terminal. Please refer to motivation recited for using applets as taught by Hickman in claim 1.

8. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley in view of Hickman as applied to claim 1 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography", Section 9.6).

a. Regarding claim 6, Baltzley does not disclose: (m) downloading a hashing applet resident on the server into random access memory on the first local terminal; (n) creating a hash of the encrypted data document using the hashing applet on the first

Art Unit: 2132

local terminal; (o) uploading the hash of the encrypted data document from the first local terminal to the server via the network; (p) downloading the hash of the encrypted data document from the server to the second local terminal via the network; (q) downloading the hashing applet resident on the server into random access memory on the second local terminal; (r) creating a second hash of the downloaded encrypted data document using the hashing applet on the second local terminal; (s) comparing the first hash of the encrypted data document and the second hash of the downloaded encrypted data document on the second local terminal; and (t) displaying an error message on the second local terminal if the first hash of the encrypted data document does not match the second hash of the downloaded encrypted data document.

Menezes discloses creating a hash value of the encrypted message at the sender's terminal, transmitting the hash value with the encrypted message, creating a second hash value at the recipient's terminal, comparing the first hash value and the second hash value at the recipient's terminal, and informing the recipient of the result (p. 367, see 9.87 Remark, computing a MAC over the ciphertext). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method to create a hash value of the encrypted message at the sender's terminal, transmit the hash value with the encrypted message, create a second hash value at the recipient's terminal, compare the first hash value and the second hash value at the recipient's terminal, and inform the recipient of the result, as taught by Menezes, in order to allow message authentication without knowledge of the plaintext.

Hickman discloses that applets are small programs designed for a specific task (col. 2, lines 53-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method Baltzley and Menezes such that an applet is used to perform the specific task, as taught by Hickman, the specific task being creating a hash value of the encrypted message and authenticating the encrypted message using the hash value. Accordingly, the applet needs to be downloaded from the server by both the first and second terminals. Please refer to motivation recited for using applets as taught by Hickman in claim 1.

b. Regarding claim 7, Baltzley does not disclose: (u) deleting the hashing applet from the random access memory on the first local terminal; and (v) deleting the hashing applet from the random access memory on the second local terminal. Hickman discloses the applet being deleted from the terminal on termination of the applet (col. 2, lines 55-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method such that it further comprises (u) deleting the hashing applet from the random access memory on the first local terminal; and (v) deleting the hashing applet from the random access memory on the second local terminal, as taught by Hickman. Please refer to motivation recited for using applets as taught by Hickman in claim 1.

9. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley, Hickman and Menezes as applied to claim 6 above, and further in view of Moy (5,425,102) and Menezes et al. ("Handbook of Applied Cryptography", Section 10.2).

Art Unit: 2132

a. Regarding claim 8, Baltzley, Hickman and Menezes do not disclose: (w) designating a keyword on the first local terminal; (x) creating a hash of the keyword using the hashing applet on the first local terminal; (y) encrypting the data document in step (d) using the hash of the keyword as an encryption key; (z) creating a keyphrase as a clue to the keyword; (aa) communicating the keyphrase to an intended recipient of the data document; (bb) entering the keyword corresponding to the keyphrase on the second local terminal; (cc) creating a second hash of the keyword using the hashing applet on the second local terminal; (dd) decrypting the encrypted data document in step (j) using the second hash of the keyword as a decryption key.

Moy discloses designating a keyword on a first local terminal (col. 3, 33-38; col. 5, lines 25-27), encrypting data using the keyword as an encryption key (col. 3, 33-38), creating a keyphrase as a clue to the keyword (col. 5, lines 10-24; 38-46), communicating the keyphrase to an intended recipient of the data document (col. 5, lines 20-24; 38-46), entering the keyword corresponding to the keyphrase on the second local terminal (col. 5, lines 38-43), and decrypting the encrypted data using the keyword as a decryption key (col. 5, lines 40-43). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Baltzley, Hickman and Menezes such that it further comprises designating a keyword on a first local terminal, encrypting data using the keyword as an encryption key, creating a keyphrase as a clue to the keyword, communicating the keyphrase to an intended recipient of the data document, entering the keyword corresponding to the keyphrase on the second local terminal and decrypting the encrypted data using the

Art Unit: 2132

keyword as a decryption key, as taught by Moy. The motivation for doing so would have been to allow access to shared data files (col. 5, lines 25-27).

Menezes discloses creating a hash of a keyword and using the hash of the keyword as an encryption/decryption key (p. 395, 7th par., "A second technique ... a 56-bit DES key"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the combination method of Baltzley, Hickman, Menezes and Moy to create a hash of a keyword and use the hash of the keyword as an encryption/decryption key, as taught by Menezes. Accordingly, creating the hash of the keyword is performed by the hashing applet. The motivation for doing so would have been to create secret keys with sufficient entropy to provide adequate security (p. 395, 5th par).

b. Regarding claim 9, Baltzley further discloses that the first and second terminals are located in a publicly accessible location (col. 2, lines 1-4; 19-21). Baltzley does not disclose that the first or the second terminal is connected to a means for recording the data document on a tangible medium. However, Examiner takes Official Notice that the use of floppy disk drives to record data on floppy disks in computer systems is conventional and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ a floppy disk drive as a recording means for the terminals of Baltzley since Examiner takes Official Notice that the use of floppy disk drives to record data on floppy disks in computer systems is conventional and well known.

Art Unit: 2132

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley, Hickman, Menezes and Moy as applied to claim 9 above, and further in view of Nasu et al. (6,223,321). Baltzley, Hickman and Menezes do not disclose that means for recording the data document in a tangible medium includes a means for erasing, overwriting and/or destroying the data document on the tangible medium upon detection of an error or incomplete transaction. Nasu discloses a floppy disk drive including a means for correcting errors to data stored in a floppy disk upon detection of an error (col. 8, lines 27-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Baltzley, Hickman, Menezes and Moy such that the floppy disk drive including a means for correcting errors to data stored in a floppy disk upon detection of an error, as taught by Nasu, so that the cost of the floppy disk drive could be reduced (Abstract).

11. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley in view of Hickman as applied to claim 1 above, and further in view of Ginter et al. (5,982,891).

a. Regarding claim 11, Baltzley does not disclose that at least one of the first and second local terminals is located in a secured business location and connected to a means for recording the data document on a tangible medium. Ginter discloses a virtual distribution environment in which a terminal at one end of the communications channel is located in a secured business location and connected to a means for recording the data document on a tangible medium (fig. 1, element 204). It would have

Art Unit: 2132

been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method such that the one of the terminals being located in a secured business location and connected to a means for recording the data document on a tangible medium, as taught by Ginter, so that digital contents could be delivered electronically.

b. Regarding claim 12, Baltzley does not disclose delivering the data recorded on the tangible medium from the secured business location to an intended recipient.

Ginter discloses delivering the data recorded on the tangible medium from the secured business location to an intended recipient (fig. 1, element 216). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Baltzley method to deliver the data recorded on the tangible medium from the secured business location to an intended recipient, as taught by Ginter. The motivation for doing so would have been to provide alternative means of delivery.

12. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley, Hickman and Menezes (Section 9.6) as applied to claim 6 above, and further in view of Moy, Menezes (Section 10.2) and Challener et al. (6,718,468). Baltzley, Hickman and Menezes do not disclose: (w) designating a keyword on the first local terminal; (x) combining the keyword with a public or private key to create a semi-private encryption key; (y) creating a hash of the semi-private encryption key using the hashing applet on the first local terminal; (z) encrypting the data document in step (d) using the hash of the semi-private encryption key as an encryption key; (aa) creating a keyphrase as a clue to

Art Unit: 2132

the keyword; (bb) communicating the keyphrase to an intended recipient of the data document; (cc) entering the keyword corresponding to the keyphrase on the second local terminal; (dd) combining the keyword with the public or private key to recreate the semi-private encryption key; (ee) creating a second hash of the semi-private encryption key using the hashing applet on the second local terminal; (ff) decrypting the encrypted data document in step (j) using the second hash of the semi-private encryption key as a decryption key.

Moy discloses designating a keyword on a first local terminal (col. 3, 33-38; col. 5, lines 25-27), encrypting data using the keyword as an encryption key (col. 3, 33-38), creating a keyphrase as a clue to the keyword (col. 5, lines 10-24; 38-46), communicating the keyphrase to an intended recipient of the data document (col. 5, lines 20-24; 38-46), entering the keyword corresponding to the keyphrase on the second local terminal (col. 5, lines 38-43), and decrypting the encrypted data using the keyword as a decryption key (col. 5, lines 40-43). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Baltzley, Hickman and Menezes such that it further comprises designating a keyword on a first local terminal, encrypting data using the keyword as an encryption key, creating a keyphrase as a clue to the keyword, communicating the keyphrase to an intended recipient of the data document, entering the keyword corresponding to the keyphrase on the second local terminal and decrypting the encrypted data using the keyword as a decryption key, as taught by Moy. The motivation for doing so would have been to allow access to shared data files (col. 5, lines 25-27).

Menezes discloses creating a hash of a keyword and using the hash of the keyword as an encryption/decryption key (p. 395, 7th par., "A second technique ... a 56-bit DES key"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the combination method of Baltzley, Hickman, Menezes to create a hash of a keyword and use the hash of the keyword as an encryption/decryption key, as taught by Menezes. Accordingly, creating the hash values is performed by the hashing applet at both terminals. The motivation for doing so would have been to create secret keys with sufficient entropy to provide adequate security (p. 395, 5th par).

Challenger discloses combining a keyword with a private key (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Baltzley, Hickman and Menezes further to combine the keyword with a private key, as taught by Challenger. Accordingly, the hashing applet creates the hash values of the combined keyword and the private key. The motivation for doing so would have been that a user could access the user's private key to perform an authentication function by providing the pass phrase (Abstract).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cane et al (5,940,507) discloses secure file archive through encryption key management.

Smith et al (6,385,655) discloses method and apparatus for delivering documents over an electronic network.

Holloway (6,424,718) discloses a data communications system using public key cryptography in a Web environment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

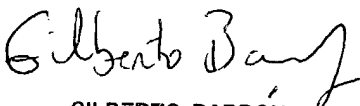
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
8/20/04


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100